REMARKS/ARGUMENTS

In the Office action mailed April 13, 2010, claims 33-39 were rejected under 35 U.S.C. § 112, second paragraph as being indefinite. In a "First ground rejection," claims 20-27, 29-31, and 33-39 were rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 5,754,938 to Herz et al. ("Herz") in view of Pfitzmann and Kohntopp, Anonymity, Unobservability, and Pseudonymity—A Proposal for Terminology, LNCS 2009 ("Pfitzmann") and further in view of further in view of Engberg and Harning, Privacy Authentication—persistent non-identification in Ubiquitous environment ("Engberg"). Claim 32 was rejected under 35 U.S.C. § 103(a) as unpatentable over Herz in view of Pfitzmann, Engberg, and U.S. Patent Pub. No. 2006/0155993 to Busboon ("Busboon"). In a "Second ground rejection," claims 20-27, 29-31, and 33-39 were rejected under 35 U.S.C. § 103(a) as unpatentable over Int'l Pub. No. WO 01/90968 to Engberg ("Engberg-1") in view of Pfitzmann. Claim 32 was rejected under 35 U.S.C. § 103(a) as unpatentable over Herz in view Pfitzmann, Busboon, and Engberg. The Examiner is thanked for careful attention to the complex application.

Claims 20-27 and 29-39 were pending in the application. Claim 20 is amended. Claims 33-39 are cancelled. Claims 40-43 are new.

Claim Amendments

Claim 20 is amended to add "said privacy reference point identified by a domain offset link and a relative reference." Support for this may be found in the original application at page 15 lines 8-13, which states, "One important aspect of this invention is the ability to establish anonymous connections between the offline world and the online world. These are called Privacy Reference Point (PRP) which are virtual addresses based on a domain offset link and a relative reference (<domain>Ref for instance http://www.PRPRef.NET/Ref# where Ref# is any combination of characters, numbers etc.)."

New Claims

Support for new claim 40 may be found throughout the application and in particular:

at page 7, lines 17-21 of the application, which states, "In addition this invention creates a generic solution as to how devices can communicate using a virtual device identity to eliminate linkability across transactions with the same device."

at page 104, lines 8-9 of the application, which states, "Ownership SSDK keys are specific and not reused across multiple tags as these are not tamper-resistant."

at page 112, lines 2-3 of the application, which states, "SSDK should NOT be reused across multiple Tags."

at page 15, lines 15-18 of the application, which states, "Whenever a transaction is initiated a PRP is provided by the Chip Card as the transaction specific identifier or one-time-only card number. Except for this identifier the Chip Card will leave NO additional identifiers unless voluntary approved by the Client as part of the transaction."

and at page 32, lines 11-23 of the application, which states, "PRPs can be generated and shared in multiple ways. ... Another way would to generate random-like input could be to use an algorithm based method using a shared secret as seed value. One such implementation could be based on a low-collusion hash of a combination of a CardRef (Chip Card specific key) and a changing part such as a counter."

Support for new claim 41 may be found throughout the application and in particular:

at page 15, lines 9-13, which states "These are called Privacy Reference Point (PRP) which are virtual addresses based on a domain offset link and a relative reference (<domain>Ref for instance http://www.PRPRef.NET/Ref# where Ref# is any combination of characters, numbers etc.)."

at page 32, lines 11-23 of the application, which states, "PRPs can be generated and shared in multiple ways. The most secure way would be to generate pure random input numbers in a secure HOME environment and share these with the Chip Card. These random numbers can be used to generate both a PRP as well as an authentication key. Another way would to generate random-like input could be to use an algorithm based method using a shared secret as seed value. One such implementation could be based on a low-collusion hash of a combination of a CardRef (Chip Card specific key) and a changing part such as a counter."

at page 15, lines 7-14 of the application, which states, "The current system relies on a permanent shared secret between the RFID reader and tag, which may introduce problems. However, we believe that the random session key can be shown to provide a good basis for changing the shared secret SSDK on a per session basis, which will

provide backward secrecy (using for instance a hash combination) and forward secrecy (an attacker needs to record every change as there is no algorithmic link between the various SSDK). Synchronisation of changing shared secrets can be established based on the acknowledgment as the coordinating mechanism."

at page 21, lines 19-23 of the application, which states, "Period-specific public keys can be published by any number of trusted parties meaning that the corresponding private key will be deleted within a pre-defined timeframe preferable in some verifiable manor using for instance verified hardware to store the keys. Since public keys are published a trusted party does not know what kind of secrets is guarded and for whom."

at page 37, lines 23-26 of the application, which states, "A command or reference could be included as a fourth parameter. One use of this is if the Tag contains multiple keys to help the key detect which key to check against in order to save power. Another is to issue specific commands such as Transfer, create new keys or open for access to authenticate hidden keys."

at page 42 lines 6-8 of the application, which states, "Such a protocol could in a preferred implementation include storing an additional Group Code (GC) stored on multiple devices and a Device Identifier (01) chosen specific by the client for the single device."

at page 54 lines 16-17 of the application, which states, "Each part publish this days (or other changing component such as an event or context specific key) version of his preferred address book relationships."

and at page 25 lines 22-24 of the application, which states, "Another solution would be to store the identifying signature key in an encrypted nonlinkable version (including salt and different hybrid encryption schemes etc.) at some or all Privacy Reference Points."

Support for new claim 44 may be found throughout the application and in particular:

in figure 16, and at page 37 lines 2-6 of the application, which states, "In the preferred solution, X1 comprises a one-way low-collusion hash algorithm such as MD5 of the combination of the device secret (OS), a random session key (R) and the timestamp

(DT2). X2 comprises the XOR combination of random session key (R) and a hash of the Device Secret (DS) and the timestamp (DT2)."

Support for new claim 45 may be found throughout the application and in particular:

in figure 16 and at page 102 lines 23-26 of the application, which states, "The product tag will remain silent, but the consumer can at any time resume control of the Product tag and integrate the product within the consumer sphere. Until then the tag appear as if it is not there - perhaps forever."

Claim 40 is novel over the referenced art for at least "without any other device in the communication network being able to distinguish between two transactions between the first device and the second device and two transactions between any other two devices in the communication network" and "independently connect to a same connection address in an address space hosted in the communication network without reusing any identifier related to the first device or the second device" which do not appear to be taught by the prior art.

Claims 41-43 depend from claim 40 and are thus novel for at least the above reasons.

Rejections under 35 U.S.C. § 112

The Office action rejected claims 33-39 as indefinite. These claims are cancelled solely to advance prosecution of the application. The right to present the same or similar claims during later prosecution of this or another application is reserved.

First ground for rejection under 35 U.S.C. § 103

The Office action rejected claims 20 as being unpatentable over Herz in view of Pfitzmann and Engberg. The rejection is respectfully traversed as follows.

Amended claim 20 recites in part "providing a privacy reference point in said data communication network, said privacy reference point configured for use in one transaction, said privacy reference point identified by a domain offset link and a relative reference."

The Office action correlates the proxy server of Herz to the "privacy reference point" specified in claim 20. Office action, p. 7. Herz describes its proxy server as "a server computer with CPU, main memory, secondary disk storage and network communication function and with a database function." Herz, col. 34, lines 27-29. Herz also states that the proxy server "provides three sorts of service to each user U in its user base": (1) "bidirectionally transfer communications between user U and other entities"; (2) "record user-specific information

associated with user U"; and (3) "act as a selective forwarding agent for unsolicited communications that are addressed to user U." Herz, col. 32, lines 18-50. However, Herz is silent on how its proxy server is identified. Thus, even if Herz's proxy server correlates to a "privacy reference point," Herz does not teach "said privacy reference point identified by a domain offset link and a relative reference," as recited in claim 20. The other art of record also does not appear to teach "said privacy reference point identified by a domain offset link and a relative reference."

Thus claim 20 recites features that are not found in the prior art and is allowable.

Claim 20 also recites "said privacy reference point configured for use in one transaction." The Office action acknowledges that this is not disclosed in Herz and points to Pfitzmann to cure this failure of Herz. Office action, p. 9. Regarding combining teachings from Herz and Pfitzmann, the Office action states, "Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the method of Herz by including the teaching of Pfitzmann because it would provide a different transaction pseudonym is used, e.g. randomly generated transaction numbers for online-banking. Thus, there is at least no possibility to link different transactions by equality of pseudonyms. Therefore, transaction pseudonyms can be used to realize as strong anonymity as possible." *Id.*

However, the combination of Herz and Pfitzmann cannot be obvious because the proposed modification of Herz would render it unsatisfactory for its intended purpose. *See* MPEP 2143.01. Herz's system relies on storing information about a user that requires reuse of pseudonyms to achieve its purpose of "customized electronic identification of desirable objects" using a "'target profile interest summary' for each user, which target profile interest summary describes the user's interest level in various types of target objects." Herz, col. 1, lines 16-26. Actions of the user are used by the Herz's system to keep the target profile interest summary "updated on a continuing basis to reflect each user' changing interests." Herz, col. 1, lines 19-65.

Reuse of pseudonyms is ubiquitous in Herz. For example, as quoted above, Herz's proxy server "record[s] user-specific information associated with user U." Furthermore, Herz explicitly requires a single pseudonym to be used repeatedly.

> From the service provider's perspective, our system provides security, in that it can guarantee that users of a service are legitimately entitled to the services used and that no user is using multiple pseudonyms to communicate with the same provider. This uniqueness of pseudonyms is important for the purposes of

> this application, since the transaction information gathered for a given individual must represent a complete and consistent picture of a single user's activities with respect to a given service provider or coalition of service providers; otherwise, a user's target profile interest summary and user profile would not be able to represent the user's interests to other parties as completely and accurately as possible.

Herz, col. 32, line 66 to col. 33, line 11 (emphasis added).

Herz also states that a "pseudonym is an artifact that allows a service provider to communicate with users and build and accumulate records of their preferences over time." Herz, col. 31, lines 48-51. Use of a pseudonym for one transaction would prevent a service provider in Herz's system from building and accumulating records over time.

Accordingly, the Office action does not make a prima facie case of obviousness based on the combination of Herz and Pfitzmann.

Thus is respectfully requested that this rejection be withdrawn with respect to claim 20 and claims 21-27 and 29-32 that depend from claim 20.

Second ground for rejection under 35 U.S.C. § 103

The Office action rejected claims 20 as being unpatentable over Engberg-1 in view of Pfitzmann. The rejection is respectfully traversed as follows.

Amended claim 20 recites in part "providing a privacy reference point in said data communication network, said privacy reference point configured for use in one transaction, said privacy reference point identified by a domain offset link and a relative reference."

Regarding the corresponding pre-amendment clause, the Office action states, "providing a privacy reference point in said data communication network, said privacy reference point configured for use in one transaction **[Engberg-1: abstract: Privacy is established using a principle of multiple *non-linkable pseudonyms or Virtual Identities (VID)*; See also pg. 35 , lines 10-23 ; Virtual Identity; pg. 33, Zero-knowledge generation of *on-time-only keys*; See also pg. 106, lines 25 to pg. 107, lines 32; *one-time-only VID*; pg. 131, lines 15-20; pg. 38]**" Office action, p. 21.

It appears that the Office action correlates the Virtual Identities (VID) of Engberg-1 to the "privacy reference point" specified in claim 20. Although it is unclear that the correlation is correct, Engberg-1 does not describe its VID as identified by a domain offset link and a relative reference. Engberg-1, like Herz, appears to be silent on how its VID is identified. Thus, Engberg-

1 does not teach "said privacy reference point identified by a domain offset link and a relative reference," as recited in claim 20. As discussed above regarding the first ground for rejection, the other art of record also does not appear to teach "said privacy reference point identified by a domain offset link and a relative reference."

Thus claim 20 recites features that are not found in the prior art and is allowable.

Claim 20 also recites "establishing a first communication path from said chip card to said privacy reference point" and "establishing a second communication path from a first communication device associated with a first entity to said privacy reference point through said data communication network." Regarding the first communication path clause, the Office action states, "Engberg-1: abstract: pg. 6, lines 3-12; providing a first virtual identifier of the first legal entity to the second legal entity, and establishing a communication path in according with a set of communication Rules specified by the first legal entity." Office action, p. 21 (bold and italics removed). Regarding the second communication path clause, the Office action identically states, "Engberg-1: abstract: pg. 6, lines 3-12; providing a first virtual identifier of the first legal entity to the second legal entity, and establishing a communication path in according with a set of communication Rules specified by the first legal entity between the first and the second legal entity." Office action, p. 23 (bold and italics removed). It is submitted that a "communication path ... between the first and the second legal entity" of Engberg-1 cannot be both the "first communication path from said chip card to said privacy reference point" and the "second communication path from a first communication device associated with a first entity to said privacy reference point through said data communication network."

Thus, Engberg-1 does not teach, alone or in combination with Pfitzmann, establishing a first communication path from said chip card to said privacy reference point" and "establishing a second communication path from a first communication device associated with a first entity to said privacy reference point through said data communication network," as recited by claim 20.

Accordingly, claim 20 is not obvious over Engberg-1 and Pfitzmann.

Thus is respectfully requested that this rejection be withdrawn with respect to claim 20 and claims 21-27 and 29-32 that depend from claim 20.

Summary

In summary, it is respectfully submitted that claims 20-27, 29-32, and 40-43 are patentable over the art of record and show be allowed. Passage of the application to issue is therefore earnestly solicited.

Respectfully submitted,

Date: April 13, 2011

Daniel L. Essig
Registration No. 61,575

Klein, O'Neill & Singh, LLP (Customer No.: 22145)
18200 Von Karman Avenue, Suite 725
Irvine, California 92612
Tel: (949) 955-1920
Fax: (949) 955 1921